

信息安全漏洞周报

2012 年 1 月 2 日-2012 年 1 月 8 日

2012 年 第 1 期

本周漏洞基本情况

本周信息安全漏洞威胁整体评价级别为低。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 41 个，其中高危漏洞 14 个、中危漏洞 27 个、低危漏洞 0 个。上述漏洞中，可利用来实施远程攻击的漏洞有 40 个。本周收录的漏洞中，已有 29 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。本周互联网上出现“WSN Links 'report.php' SQL 注入漏洞”、“Netcut ARP 拒绝服务漏洞”等的零日攻击代码，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 3 个成员单位和 2 个单位或个人报送了本周收录的全部 41 个漏洞。此外，来自上海交通大学网络信息中心的漏洞研究者报送了 MongoDB 数据库系统的默认配置管理漏洞，目前 CNVD 工作委员会在成员单位北京知道创宇公司协助下完成漏洞验证，漏洞详情将择期发布。网御星云公司报送了两起知名网站的跨站脚本漏洞事件（未收录），其中某知名微博网站跨站漏洞事件转由 CNVD 成员单位国家互联网应急中心处置。

各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、安天实验室报送数量较多。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	54	0
启明星辰	31	0
安天实验室	27	0
安氏领信	4	0
网御星云	2	0
上海交通大学	4	1
总计	41（去重）	0

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 OpenSSL Project、Apache、Drupal、Siemens 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	OpenSSL Project	6	15%
2	Apache	4	10%
3	Drupal	3	7.5%
4	Siemens	2	5%
5	Novell	2	5%
6	Google	2	5%
7	Mozilla	1	2.5%
8	Moodle	1	2.5%
9	Nginx	1	2.5%
10	FFmpeg	1	2.5%
11	其它	18	42.5%

表 2 漏洞产品涉及厂商分布统计表

本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Apache 产品安全漏洞

本周，Apache Struts 和 Geronimo 被披露存在多个安全漏洞。Apache Struts 是一款建立 Java web 应用程序的开放源代码架构软件；Apache Geronimo 是一款开源 Java 2 Platform, Enterprise Edition(J2EE)应用服务器软件。远程攻击者可以利用上述产品漏洞执行任意命令、覆盖任意文件或进行拒绝服务攻击。CNVD 收录的相关漏洞包括：Apache Geronimo Web 表单哈希碰撞拒绝服务漏洞、Apache Struts 远程命令执行漏洞（CNVD-2012-09286）、Apache Struts 任意文件覆盖漏洞、Apache Struts 远程命令执行漏洞（CNVD-2012-09285）。上述漏洞的综合评级均为“高危”。目前，除“Apache Geronimo Web 表单哈希碰撞拒绝服务漏洞”外，厂商已发布其余漏洞的补丁程序。CNVD 提醒广大 Apache 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36453
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36510
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36511
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36508

2、Siemens Tecnomatix FactoryLink 安全漏洞

Siemens Tecnomatix FactoryLink 是一款工业自动控制软件，用于监督、管理和控制工业流程。本周，Siemens Tecnomatix FactoryLink 被披露存在多个安全漏洞，远程攻击者可以利用漏洞以应用程序上下文执行任意代码或覆盖系统文件。CNVD 收录的相关漏洞包括：Siemens Tecnomatix FactoryLink ActiveX 任意文件覆盖漏洞、Siemens Tecnomatix FactoryLink ActiveX 缓冲区溢出漏洞。其中，“Siemens Tecnomatix FactoryLink ActiveX 缓冲区溢出漏洞”的综合评级为“高危”。目前，厂商已发布这些漏洞的修补程序，CNVD 提醒广大用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36516

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36528

3、Novell Netware 安全漏洞

Novell Netware 是一款网络操作系统。本周，Novell Netware 存在多个远程代码执行漏洞。远程攻击者可以利用漏洞执行任意代码。CNVD 收录的相关漏洞包括：Novell Netware XNFS.NLM STAT Notify 远程代码执行漏洞、Novell Netware XNFS.NLM NFS 重命名远程代码执行漏洞。上述漏洞的综合评级均为“高危”。目前，Novell 已经发布上述漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36690

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36688

4、OpenSSL 产品安全漏洞

OpenSSL 是一款开放源码的基于 SSL 的安全软件，用来实现网络通信的高强度加密。本周，OpenSSL 被披露存在多个漏洞。远程攻击者可以利用漏洞获得敏感信息，进行拒绝服务攻击或破坏应用程序。CNVD 收录的相关漏洞包括：OpenSSL 存在多个漏洞（CNVD-2012-09307、CNVD-2012-09308、CNVD-2012-09309、CNVD-2012-09310、CNVD-2012-09311、CNVD-2012-09312）。目前，厂商已经发布上述漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36636

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36648

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36653

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36650

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36652

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36649

5、WSN Links 'report.php' SQL 注入漏洞

WSN Links 是一款基于 PHP/MySQL 的检索脚本软件。本周，WSN Links 被披露存在一个 SQL 注入漏洞。由于'report.php'脚本未能正确处理用户提交的输入，远程攻击者可以利用漏洞进行 SQL 注入攻击，获得数据库敏感信息或控制应用系统。该漏洞的

综合评级为“高危”，且攻击代码已在互联网出现，主要影响 WSN Links 6.2.25/6.0.1/5.1.51/5.1.49/5.0.81/4.0.34P 多个版本。目前，厂商尚未发布此漏洞的修补程序，CNVD 提醒广大用户随时关注厂商主页以获取最新版本。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36451

更多高危漏洞如表 3 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。

参考链接：<http://www.cnvd.org.cn/publish/main/52/index.html>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2012-09305	Pligg CMS 'status'参数 SQL 注入漏洞	高	用户可下载最新版本的 Pligg: http://pligg.svn.sourceforge.net/viewvc/pligg/trunk/search.php?r1=2255
CNVD-2012-09301	FFmpeg SVQ1 流文件远程代码执行漏洞	高	Ubuntu linux 用户可参考如下安全公告获得补丁程序: http://permalink.gmane.org/gmane.linux.ubuntu.security.announce/1572
CNVD-2012-09313	PHPIDS ReDoS 过滤器安全绕过漏洞	高	PHPIDS 0.7 已经修复此漏洞，建议用户下载使用： https://www.phpids.org/
CNVD-2012-09278	Posse Softball Director CMS(team.php) SQL 盲注漏洞	高	暂无
CNVD-2011-09252	VLC Media Player TiVo Demuxer 远程堆缓冲区溢出漏洞	高	VideoLAN VLC media player 1.1.13 已经修复此漏洞，建议用户下载使用： http://www.videolan.org/

表 3 部分高危漏洞列表

小结：本周，Apache Struts 和 Geronimo 被披露存在多个安全漏洞。远程攻击者可以利用漏洞执行任意命令、覆盖任意文件或造成拒绝服务攻击。这两款软件在国内政府、企业以及个人网站中均应用较多。此外，Siemens 工控软件、Novell 操作系统和 OpenSSL 应用程序存在的多个安全漏洞，这些应用于专用领域的软件漏洞会对企业信息化应用安全构成威胁。

此外，使用 WSN Links 检索脚本的用户需注意防范该产品本周出现的零日漏洞，防范由此诱发的注入攻击。

CNVD 提醒使用上述软件的相关机构和个人及时采取安全防范措施。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Drupal 发布升级程序，修补多个安全漏洞

Drupal 是一款开源的内容管理系统 (CMS)。本周, Drupal 发布升级程序, 修补了 Fill PDF 模块和 Registration Codes 模块多个安全漏洞, 避免远程攻击者可以绕过安全限制或执行任意代码。CNVD 已收录相关补丁, 请广大用户及时下载更新, 避免引发漏洞相关的安全事件。

补丁下载链接:

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=7054

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=7112

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=7111

本周要闻速递

1. 新浪爱问用户信息泄露 官方承认存在漏洞

近日, 某安全网站曝出新浪爱问存在安全漏洞, 可能导致众多新浪用户的账户密码泄露, 并可能导致用户新浪微博被盗取。新浪随后发布公告表示, 目前已紧急修复了这一漏洞, 并对这一漏洞可能导致信息泄露的 30 万新浪账号进行了保护。新浪爱问存在一个 sql 注射型漏洞, 黑客可以利用这一漏洞直接读取爱问的数据库内容, 包括明文密码在内的 7000 多万新浪用户信息存在被盗风险。而且因为部分用户的爱问账号与新浪微博账号存在关联, 用户的新浪微博也存在风险。漏洞信息公布后, 新浪也马上发布了公告进行回应, 承认新浪爱问存在系统漏洞, 并表示新浪爱问存在的这一漏洞已被修复。

参考链接: <http://tech.qq.com/a/20120106/000092.htm>

2. 微软 1 月将发 7 个补丁 修复 Windows 等产品漏洞

据国外媒体报道, 微软计划在 2012 年的第一个补丁星期二发布 7 个补丁, 修复 Windows 操作系统和微软开发工具以及软件中的安全漏洞。据微软周四发布的提前通知称, 微软将修复包括 Windows 7 和 Windows Server 2008 R2 在内的所有版本的 Windows 中的安全漏洞。在这 7 个补丁中只有 1 个是“严重”等级的, 其余的都是“重要”等级的补丁。这个“严重”等级的补丁修复媒体播放器软件中的一个远程执行代码漏洞。对于 Windows 7 和 Windows 2008 R2 用户来说, 这个补丁可以降为“重要”等级。微软将在 1 月 10 日的补丁星期二发布这些补丁。这些补丁有 6 个修复各种版本的 Windows 的漏洞, 只有一个修复微软开发工具的漏洞。Windows 7 和 Windows 2008 R2 的安全漏洞少一些, 因为有两个补丁不适用这两个软件。安全专家表示, BEAST 工具、各种泄露信息的攻击和升级权限的问题都可以利用这些安全漏洞。微软还将更新其结构化异常处理覆写保护技术。这是一种纵深防御功能, 使攻击者很难成功地利用老式应用程序的安全漏洞。

参考链接: http://news.ccidnet.com/art/946/20120106/3500227_1.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家互联网应急中心的全称是国家计算机网络应急技术处理协调中心（英文简称是 CNCERT 或 CNCERT/CC）成立于 1999 年 9 月，是工业和信息化部领导下的国家级网络安全应急机构，致力于建设国家级的网络安全监测中心、预警中心和应急中心，以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，支持基础信息网络的安全防护和安全运行，支援重要信息系统的网络安全监测、预警和处置；国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999